REMARKS

Explanation of Amendments

Claims 3, 6, 7, 9, 10, 12, 19, and 20 have been amended for clarification. Claims 1-2 and 13-18 have been canceled as non-elected claims. Claims 22-28 have been added as system claims for implementing the method of claims 3, 5-12, and 19-21. No new matter has been entered and no new issues have been raised. Upon entry of the above amendments, claims 3, 5-12, and 19-28 and will be pending.

Claim Rejections – 35 USC §103

Claims 3, 6-7, 9 and 21 stand finally rejected under 35 USC §103(a) as allegedly being unpatentable as obvious over Cheriton (US 7,120,931) in view of Vaidya (US 6,279,113). Claims 5 and 8 stand finally rejected under 35 USC §103(a) as allegedly being unpatentable as obvious over Cheriton and Vaidya in view of Desai et al. (US 2003/0188189). Claims 10 and 12 stand finally rejected under 35 USC §103(a) as allegedly being unpatentable as obvious over Cheriton and Vaidya in view of Daizo (US 6,424,654). Claim 11 stands finally rejected under 35 USC §103(a) as allegedly being unpatentable as obvious over Cheriton, Vaidya, and Daizo in view of Desai et al. Claim 19 stands finally rejected under 35 USC §103(a) as allegedly being unpatentable as obvious over Cheriton and Vaidya in view of Trcka et al. (US 6,453,345). Finally, claim 20 stands finally rejected under 35 USC §103(a) as allegedly being unpatentable as obvious over Cheriton and Vaidya in view of Ullmann et al. (US 2002/0174362). These rejections are respectfully traversed.

As noted in the previous amendment response, the claimed method detects malicious activity on a communications network, including attacks such as those that are intended to secure proprietary information or interfere with the operation of a computer, as well as probes and scans that typically precede such an attack. In particular, the claimed method recites a method of detecting surveillance probes on a computer communications network, comprising:

> receiving a plurality of messages from a data sensor, located at a network audit point, that samples data packets on said computer communications network and outputs said messages, each of said messages describing an event occurring on said communications network;

> processing said messages to form extrapolated connection sessions from said sampled data packets by clustering packets a) exchanged between two addresses within a specified time period where the addresses are not predetermined or (b) having certain flags set or c) having addresses that are not predetermined but have similar characteristics; and
>
> detecting a surveillance probe by:
> grouping connection sessions into a plurality of groups;
> scoring each group; and
> generating an alert for each group whose score is greater than an empirically derived threshold.

New claim 22 recites a system that implements the claimed method using a detector and a processor. Such a method and system are not shown or suggested by the cited prior art references.

Cheriton discloses a system and method for analyzing high speed data entering a router or firewall to identify detailed characteristics of the packets involved in an attack or a failure. The method includes generating filters based on analyzed flow data by separating the data into different network flows, analyzing at least one of the network flows, and detecting potentially harmful network flows. A filter is generated to prevent packets corresponding to the detected potentially harmful network flows from passing through the network device. As illustrated in Figures 3 and 4, a netflow mechanism processes each packet in the network flow responsive to the entry for the network flow in the flow cache, and the netflow mechanism implements administrative policies that are designated for each network flow rather than for each packet. The network flows are analyzed and information on incoming packets is provided without examining each packet received. This "flow collection aggregation" allows for data to be stored by aggregate summary records instead of raw data records (column 6, lines 56-65). Once a group of packets is identified as harmful, the corresponding network flows may be analyzed to further refine the filter. The flow analyzer monitors the statistics associated with the aggregate filters and, if the statistics associated with an aggregate filter entry indicate a potential problem, creation of netflow entries is enabled for packets matching the entry. The flow analyzer receives a flow record for each flow matching the aggregate, and the flow generator determines how to refine the aggregate filter.

Claim 3 includes the step of "receiving a plurality of messages from a data sensor, located at a network audit point, that samples data packets on said computer communications network and outputs said messages, each of said messages describing an event occurring on said communications network." In rejecting claim 3 over Cheriton, the Examiner alleged that Cheriton discloses receiving a plurality of messages from a data sensor located at a network audit point, where each of the messages describes an event occurring on the communications network as claimed. The Examiner is mistaken. Cheriton does not disclose a data sensor that samples data packets and outputs messages describing events, such as IP connections, as claimed. A router clearly is not a data sensor that outputs messages describing an event such as an IP connection. Moreover, the data processed by Cheriton is not sampled data describing events. On the contrary, Cheriton provides the network flow directly into the ACL classification element 80 and netflow lookup 82 as illustrated in Figure 3. No data sampling by a data sensor and no processing of messages representing network events are taught.

Moreover, Cheriton does not teach processing messages describing an event to form extrapolated connection sessions from the sampled data packets. On the contrary, Cheriton sorts the network flow into flows (or buckets) 86 as shown in Figure 3. Since Cheriton does not sample the network data but instead processes the entire network flow, no "extrapolated connection sessions" are generated as claimed.

Cheriton also does not detect a surveillance probe by grouping connection sessions into a plurality of groups. Furthermore, as acknowledged by the Examiner, Cheriton does not score each group or generate an alert for each group whose score is greater than an empirically derived threshold. For a teaching of scoring each group and generating an alert for each group whose score is greater than an empirically derived threshold, the Examiner references Vaidya's teachings of counting characteristics in the packet stream, such as an attempt to access a file, and determining whether the count exceeds a threshold. The Examiner's reliance upon Vaidya is misplaced.

As noted in the previous response, Vaidya discloses a signature inspection-based network intrusion detection system that detects attacks by comparing activity on the communications network with predetermined signature profiles stored in the system. Applicant submits that Vaidya does not teach the features noted above that are not taught by Cheriton. Accordingly, even if the teachings of Vaidya could have been combined with the teachings of Cheriton as the Examiner alleges, the claimed invention would not have resulted. Withdrawal of the rejection of claim 3 is thus solicited.

Desai et al., Daizo, Trcka et al., and Ullmann et al. have been cited by the Examiner with respect to particular features of the dependent claims. Applicant submits that none of these patent documents teaches the afore-mentioned features of claim 3 that are not taught by Cheriton or Vaidya. Accordingly, even if the teachings of one or more of these references would have been combined with the teachings of Cheriton and Vaidya as the Examiner alleges, the features of claim 3 still would not have been suggested to one skilled in the art.

For at least the foregoing reasons, claim 3 and the claims dependent thereon (claims 5-12 and 19-21) are believed to be allowable over all of the cited references in any proposed combination. Moreover, new claims 22-28 are believed to be allowable for the same reasons as claim 3. Allowance of claims 3, 5-12, and 19-28 is solicited.

Conclusion

Claims 3, 5-12, and 19-28 are believed to be novel and non-obvious over the cited references. Withdrawal of all rejections and issuance of a Notice of Allowability are solicited.

Date: Monday, September 15, 2008

/**Michael P. Dunnam**/
Michael P. Dunnam
Registration No. 32,611

Woodcock Washburn LLP
Cira Centre
2929 Arch Street, 12th Floor
Philadelphia, PA 19104-2891
Telephone: (215) 568-3100
Facsimile: (215) 568-3439